Aniket Kate

Department of Computer Science
Purdue University
https://www.cs.purdue.edu/homes/akate/
aniket@purdue.edu

305 N. University Street
West Lafayette, IN
USA 47907
Office: +1-765-496-2763

EDUCATION

University of Waterloo — Waterloo, Canada
Ph.D. in Computer Science — Sep 2006–Jun 2010
Advisor: *Ian Goldberg*

Indian Institute of Technology (IIT)—Bombay — Mumbai, India
M.Tech. in Computer Science and Engineering — Aug 2004–Jun 2006

Mumbai University — Mumbai, India
B.E. in Information Technology — Aug 1999–Jul 2003

RESEARCH INTEREST

I design, implement, and analyze privacy, accountability and transparency enhancing technologies. My research integrates cryptography, distributed systems, and hardware-assisted security.

RESEARCH EXPERIENCE

Computer Science, Purdue University — West Lafayette, IN, USA
Assistant Professor — Aug 2015–*present*

Cluster of Excellence, Saarland University — Saarbruecken, Germany
Junior Faculty Member — Aug 2012–Sep 2015

Max Planck Institute for Software Systems (MPI-SWS) — Saarbruecken, Germany
Postdoctoral Researcher with Michael Backes — Sep 2010–July 2012

University of Waterloo — Waterloo, Canada
Research Assistant with Ian Goldberg — May 2007–Aug 2010
Research Assistant with Urs Hengartner — Sep 2006–Apr 2007

SELECTED ONGOING PROJECTS

- **Cryptocurrencies and Payment Networks**
  Analyze and improve the privacy and security properties of cryptocurrencies (e.g., Bitcoin) and IOU credit networks (e.g., Ripple); Develop innovative (payment/smart) contracts for interesting real-world applications.
  Work published at ESORICS'14, NDSS'15, CCS'15, PETS'16, and NDSS'17.
- **Analyzing and Improving Anonymous Communication Networks**
  Develop a framework (AnoA) for defining, analyzing, and quantifying anonymity properties for ACNs, and assess the real-time anonymity of the Tor network
  Work published at CSF'12 '13, CCS'14, and in JPC
- **Cryptography for Anonymity**
  Develop cryptographic primitives to enhance privacy, scalability, efficiency, and accountability of anonymous communication and anonymous storage protocols
  Work published at PETS'07, FC'10, WPES'12, ACNS'14 '15, ESORICS'16, NDSS'17 and in TISSec.
- **Transparency Enhancing Technologies**
  Design secure data transfer architecture (Lime) facilitating transparency in malicious data lineage scenarios; Develop tampering detection approach allowing social network operators to detect computations manipulated by Sybil attacks.
  Work published at COSN'15 and in TDSC

◇ **Longitudinal Privacy and Right to Delete/Conceal**
Analyze users' deletion habits on the online platform and the associated Streisand effect; Propose effective countermeasures to protect those deletions from the Cyberstalkers.
Work published at SOUPS'16 and in Internet Computing

◇ **Using Trusted Hardware for Privacy-preserving Distributed Systems**
Demonstrate the utility of trusted hardware towards solving the problem of privacy-preserving online advertising, and towards improving the resiliency of distributed protocol in the form of non-equivocation
Work published as Oakland'12, PODC'12 '14, and NDSS'15

REFEREED PUBLICATIONS

My advisee are underlined for clarity.

JOURNAL/MAGAZINE ARTICLES AND BOOK CHAPTERS

1 "Longitudinal Privacy Management in Social Media: The Need for Better Controls"
Mainack Mondal, Johnnatan Messias, Saptarshi Ghosh, Krishna P. Gummadi, and Aniket Kate
To appear in *IEEE Internet Computing (***IC**), 2017

2 "AnoA: A Framework for Analyzing Anonymous Communication Protocols"
Michael Backes, Aniket Kate, Praveen Manoharan, Sebastian Meiser, and Esfandiar Mohammadi
To appear in *Journal of Privacy and Confidentiality (***JPC**), 2016

3 "Data Lineage in Malicious Environments"
Michael Backes, Niklas Grimm, and Aniket Kate
*IEEE Transactions on Dependable and Secure Computing (***TDSC**), 13(2): 178-191, 2016

4 "Achieving Optimal Utility for Distributed Differential Privacy Using Secure Multiparty Computation"
Fabienne Eigner, Aniket Kate, Matteo Maffei, Francesca Pampaloni, and Ivan Pryvalov
Book chapter, *Applications of Secure Multiparty Computation*, IOS CISS, 13(5), 2015

5 "Towards Practical Communication in Byzantine-Resistant DHTs"
Maxwell Young, Aniket Kate, Ian Goldberg, and Martin Karsten
*IEEE/ACM Transactions on Networking (***ToN**), 21(1), Feb 2013

6 "Generalizing Cryptosystems Based on the Subset Sum Problem"
Aniket Kate and Ian Goldberg
*Springer International Journal of Information Security (***IJIS**)*, 10 (3)*, May 2011

7 "Pairing-Based Onion Routing with Improved Forward Secrecy"
Aniket Kate, Gregory M. Zaverucha, and Ian Goldberg
*ACM Transactions on Information and System Security (***TISSEC**)*, 13(4)*, Dec 2010

CONFERENCE PUBLICATIONS

8 "P2P Mixing and Unlinkable Bitcoin Transactions"
Tim Ruffing, Pedro Moreno-Sanchez, and Aniket Kate
To appear at *Network and Distributed System Security Symposium (***NDSS**), Feb 2017

9 "SilentWhispers: Enforcing Security and Privacy in Decentralized Credit Networks"
Giulio Malavolta, Pedro Moreno-Sanchez, Aniket Kate, and Matteo Maffei
To appear at *Network and Distributed System Security Symposium (***NDSS**), Feb 2017

10 "Anonymous RAM"
Michael Backes, Amir Herzberg, Aniket Kate, and Ivan Pryvalov
21st *European Symposium on Research in Computer Security (***ESORICS**), Sep 2016

11 "Listening to Whispers of Ripple: Linking Wallets and Deanonymizing Transactions in the Ripple Network"
Pedro Moreno-Sanchez, Muhammad Bilal Zafar, and Aniket Kate
*Privacy Enhancing Technologies Symposium (***PETS**), Jun 2016

12 "Forgetting in Social Media: Understanding and Controlling Longitudinal Exposure of Socially Shared Data"
Mainack Mondal, Johnnatan Messias, Saptarshi Ghosh, Krishna P. Gummadi, and Aniket Kate
*USENIX Symposium on Usable Privacy and Security (***SOUPS**), Jun 2016

13 "Strength in Numbers: Robust Tamper Detection in Crowd Computations"
Bimal Viswanath, Muhammad Ahmad Bashir, Muhammad Bilal Zafar, Simon Bouget, Saikat Guha, Krishna P. Gummadi, Aniket Kate, and Alan Mislove
*ACM Conference on Online Social Networks (***COSN)**, Nov 2015

14 "Liar, Liar, Coins on Fire!: Penalizing Equivocation By Loss of Bitcoins"
Tim Ruffing, Aniket Kate, and Dominique Schroeder
22^{nd} *ACM Conference on Computer and Communications Security (***CCS)**, Oct 2015

15 "Post-Quantum Forward Secure Onion Routing (Future Anonymity in Today's Budget)"
Satrajit Ghosh and Aniket Kate
13^{th} *International Conference on Applied Cryptography and Network Security (***ACNS)**, June 2015

16 "Secrecy without Perfect Randomness: Cryptography with (Bounded) Weak Sources"
Michael Backes, Aniket Kate, Sebastian Meiser, and Tim Ruffing
13^{th} *International Conference on Applied Cryptography and Network Security (***ACNS)**, June 2015

17 "Visigoth Fault Tolerance"
Daniel Porto, Joao Leitao, Cheng Li, Allen Clement, Aniket Kate, Flavio Junqueira, and Rodrigo Rodrigues
*European Conference on Computer Systems (***EuroSys)**, April 2015

18 "Privacy Preserving Payments in Credit Networks"
Pedro Moreno-Sanchez, Aniket Kate, Matteo Maffei, and Kim Pecina
*Network and Distributed System Security Symposium (***NDSS)**, Feb 2015

19 "Privacy-preserving Data Aggregation with Optimal Utility"
Fabienne Eigner, Aniket Kate, Matteo Maffei, Francesca Pampaloni, and Ivan Pryvalov
30^{th} *Annual Computer Security Applications Conference (***ACSAC)**, Dec 2014

20 "(Nothing else) MATor(s): Monitoring the Anonymity of Tor's Path Selection"
Michael Backes, Aniket Kate, Sebastian Meiser, and Esfandiar Mohammadi
21^{st} *ACM Conference on Computer and Communications Security (***CCS)**, Nov 2014

21 "CoinShuffle: Practical Decrentralized Coin Mixing for Bitcoin"
Tim Ruffing, Pedro Moreno-Sanchez, and Aniket Kate
19^{th} *European Symposium on Research in Computer Security (***ESORICS)**, Sep 2014

22 "Asynchronous MPC with a Strict Honest Majority Using Non-equivocation"
Michael Backes, Fabian Bendun, Ashish Choudhury, and Aniket Kate
33^{rd} *ACM Symposium on Principles of Distributed Computing (***PODC)**, July 2014

23 "Introducing Accountability to Anonymity Networks"
Michael Backes, Jeremy Clark, Peter Druschel, Aniket Kate, and Milivoj Simeonovski
12^{th} *International Conference on Applied Cryptography and Network Security (***ACNS)**, June 2014

24 "AnoA: A Framework For Analyzing Anonymous Communication Protocols"
Michael Backes, Aniket Kate, Praveen Manoharan, Sebastian Meiser, and Esfandiar Mohammadi
26^{th} *IEEE Computer Security Foundations Symposium (***CSF)**, June 2013

25 "Asynchronous Computational VSS with Reduced Communication Complexity"
Michael Backes, Amit Datta, and Aniket Kate
*Cryptographers' Track - RSA Conference (***CT-RSA)**, Feb 2013

26 "On the (Limited) Power of Non-Equivocation"
Allen Clement, Flavio Junqueira, Aniket Kate, and Rodrigo Rodrigues
31^{st} *ACM Symposium on Principles of Distributed Computing (***PODC)**, Jul 2012

27 "Provably Secure and Practical Onion Routing"
Michael Backes, Ian Goldberg, Aniket Kate, and Esfandiar Mohammadi
25^{th} *IEEE Computer Security Foundations Symposium (***CSF)**, Jun 2012

28 "ObliviAd: Provably Secure and Practical Online Behavioral Advertising"
Michael Backes, Aniket Kate, Matteo Maffei, and Kim Pecina
33^{rd} *IEEE Symposium on Security and Privacy (***Oakland)**, May 2012

29 "Adding Query Privacy to Robust DHTs"
Michael Backes, Ian Goldberg, Aniket Kate, and Tomas Toft
7^{th} *ACM Symposium on Information, Computer and Communications Security (***ASIACCS)**, May 2012

30 "Computational Verifiable Secret Sharing Revisited"
Michael Backes, Aniket Kate, and Arpita Patra
17^{th} *International Conference on the Theory and Application of Cryptology (***ASIACRYPT)**, Dec 2011

31 "Constant-Size Commitments to Polynomials and Their Applications"
Aniket Kate, Gregory M. Zaverucha, and Ian Goldberg
16^{th} *International Conference on the Theory and Application of Cryptology (***ASIACRYPT)**, Dec 2010

32 "Distributed Private-Key Generators for Identity-Based Cryptography"
Aniket Kate and Ian Goldberg
7^{th} *Conference on Security and Cryptography for Networks (***SCN)**, Sep 2010

33 "Practical Robust Communication in DHTs Tolerating a Byzantine Adversary"
Maxwell Young, Aniket Kate, Ian Goldberg, and Martin Karsten
30^{th} *International Conference on Distributed Computing Systems (***ICDCS)**, Jun 2010

34 "Using Sphinx to Improve Onion Routing Circuit Construction"
Aniket Kate and Ian Goldberg
14^{th} *International Conference on Financial Cryptography and Data Security (***FC)**, Jan 2010

35 "Distributed Key Generation for the Internet"
Aniket Kate and Ian Goldberg
29^{th} *International Conference on Distributed Computing Systems (***ICDCS)**, Jun 2009

36 "Anonymity and Security in Delay Tolerant Networks"
Aniket Kate, Gregory M. Zaverucha, and Urs Hengartner
3^{rd} *International Conf. on Security and Privacy in Communication Networks (***SecureComm)**, Sep 2007

37 "Pairing-Based Onion Routing"
Aniket Kate, Gregory M. Zaverucha, and Ian Goldberg
7^{th} *Privacy Enhancing Technologies Symposium (***PET)**, Jun 2007

WORKSHOP PUBLICATIONS AND THESES

38 "Lime: Data Lineage in the Malicious Environment"
Michael Backes, Niklas Grimm, and Aniket Kate
10^{th} *International Workshop on Security and Trust Management (***STM)**, Sep 2014

39 "Identity-Based Steganography and Its Applications to Censorship Resistance"
Tim Ruffing, Jonas Schneider, Aniket Kate
6^{th} *Workshop on Hot Topics in Privacy Enhancing Technologies (***HotPETs)**, Jul 2013

40 "Ace: An Efficient Key-Exchange Protocol for Onion Routing"
Michael Backes, Aniket Kate, and Esfandiar Mohammadi
11^{th} *ACM Workshop on Privacy in the Electronic Society (***WPES)**, Oct 2012

41 Aniket Pundlik Kate: "Distributed Key Generation and Its Applications"
PhD Thesis, University of Waterloo, Jun 2010

42 Aniket Kate: "Frobenius Endomorphism Based Cryptosystems"
Master Thesis, Indian Institute of Technology (IIT)—Bombay, Jun 2006

PREPRINTS AND SUBMISSIONS

43 "cMix: Anonymization by High-Performance Scalable Mixing"
David Chaum, Farid Javani, Aniket Kate, Anna Krasnova, Joeri de Ruiter, and Alan T. Sherman
Under submission, Available as *IACR Cryptology ePrint Archive Report: 2016-008*, Jan 2016
This work recently appeared in WIRED and in Fortune magazines.

44 "Encrypting Messages for Incomplete Webs of Trust"
Sanjit Chatterjee, Deepak Garg, Aniket Kate, and Tobias Theobald
Under submission, Jan 2016

45 "ClearChart: Ensuring Integrity of Consumer Ratings in Online Marketplaces"
Uzair Mahmood, Pedro Moreno-Sanchez and Aniket Kate
Under submission, Jan 2016

SELECTED INVITED TALKS

- ◇ "Keynote: Distributed IOweYou Credit Networks" at International Conference on Distributed Computing and Networking (ICDCN), Hyderabad, India. Jan 2017.
- ◇ "Tutorial: An Introduction to Credit Networks" at ACM Conference on Computer and Communications Security (CCS), Vienna, Austria. Oct 2016.
- ◇ "Distributed IOweYou Credit Networks" at Workshop on Distributed Cryptocurrencies and Consensus Ledgers (DCCL 2016), co-located with PODC 2016. July 2016
- ◇ "Enabling trust with privacy in virtual marketplaces using credit networks" at Computer Science (CS) Colloquium Series, Indiana University, Bloomington. Apr 2016
- ◇ "(Working group) Genome Privacy: Architecture and middleware" at Dagstuhl Seminar 15431, Dagstuhl, Germany. Oct 2015
- ◇ "Future Anonymity in Today's Budget" at NIST Workshop on Cybersecurity in a Post-Quantum World (NIST PQC), Gaithersburg, USA. Apr 2015
- ◇ "A little trusted hardware can go a long way towards privacy" at CASED, TU Darmstadt, Germany. Mar 2015
- ◇ "Anonymous Communication Networks: Design, Analysis and Challenges" at TU Dresden, Germany. Sep 2014
- ◇ "Differential Guarantees for Cryptographic Systems" at Microsoft Research, India. Apr 2014
- ◇ "Asynchronous MPC with a Strict Honest Majority Using Non-equivocation" at Applied Multi-Party Computation Workshop, Microsoft Research, Redmond, USA. Feb 2014
- ◇ "Introducing Accountability to Onion Routing" at *Grande Region Security and Reliability Day (GRSRD 2013)*. Apr 2013
- ◇ "Towards Practical and Efficient Distributed Trust" at *Indian Institute of Technology-Kharagpur (IIT-Kgp)*, India. Sep 2012
- ◇ "An Interplay between Anonymity, Privacy, and Accountability" at *Indian Statistical Institute (ISI), Kolkata*, India. Sep 2012
- ◇ "Recent Improvements to Onion Routing" at *IBM Research - Zurich*, Rueschlikon, Switzerland. Jan 2012
- ◇ "Recent Improvements in Onion Routing Circuit Construction" in the *Laboratory of Algorithmics, Cryptology and Security (LACS), University of Luxembourg*, Luxembourg. Feb 2010
- ◇ "Anonymous Key Agreement in an Identity-based Infrastructure and Applications" at the *MITACS 2009 Annual Conference*, Canada. Jun 2009

SUPERVISION EXPERIENCE

PhD Candidates

1 Tim Ruffing (@Saarland University, Germany) Summer 2013–Spring 2017
Topic: Cryptocurrencies: Science and Applications

2 Pedro Moreno-Sanchez Winter 2013/14–Fall 2017
Topic: IOweYou Credit Network Systems

3 Sze Yiu Chau (with Ninghui Li) Fall 2015–*Spring 2018*
Topic: Formal Analysis of Real-World Security Protocols

4 Mohsen Minaei Fall 2015–*Fall 2018*
Topic: Right to be Forgotten

5 Debajyoti Das — Fall 2015–*Spring 2020*
Teaching Assistant, Qual I in progress

Graduate Advisees

5 Duc V Le (with Mikhail Atallah) — Fall 2015–*Spring 2020*
Teaching Assistant, Qual I in progress

6 Easwar V Mangipudi — Fall 2015–*Spring 2020*
Teaching Assistant, Qual I in progress

Master Thesis Students

1 Siddharth Gupta — Spring 2016–present
2 Simon Heinzel (@Saarland University) — Summer 2015–Winter 2015/16
3 Tobias Theobald (@Saarland University) — Summer 2015–Winter 2015/16
4 Uzair Mahmood (@Saarland University) — Winter 2014/15–Summer 2015
5 Ivan Pryvalov (@Saarland University) — Summer 2013–Summer 2014

Bachelor Thesis Student

1 Niklas Grimm (@Saarland University) — Winter 2012/13

Teaching Experience

Purdue University

(CS 528) Network Security — Spring 2016, 2017
(CS 426) Computer Security — Fall 2016
(CS 699) Hot Topics in Privacy Enhancing Technologies — Fall 2015

Saarland University

Advanced Course: Applied Cryptography — Winter 2014/15
Seminar: Practical Cryptographic Systems — Winter 2012/13, Summer 2014
Advanced Course: Privacy Enhancing Technologies (co-taught) — Summer 2013, 2014, 2015

Professional Activities

◇ Program Committee Member:
@Purdue University
CSF 2017, POST 2017, Eurocrypt 2016. ICDCS 2016-17. UEOP 2016. FC 2016. Bitcoin 2016-17. ACNS 2016. ACM CCSW 2015. ACM WPES 2015.

@Saarland University
IEEE CloudCom 2015. FCS 2015. ICDCS 2015. ICWE 2015. CPSS 2015. HotPETS 2014. ProvSec 2014-15. WWW 2013. SPACE 2013-14. ACM WPES 2012.

◇ Conference Leadership:
Poster/Demo co-Chair — ACM CCS 2016

◇ External Reviewer (Journals):
ACM TISSec. Computer Security. ACM TWEB. IEEE Information Theory. Designs, Codes and Cryptography (DCC). IEEE TIFS. IEEE TDSC. Distributed Computing (DC). IEEE TPDS. IEEE Transactions on Computers (ToC). Information Processing Letters (IPL). Acta Informatica.

◇ Bitcoin Foundation Grant Committee — 2014

◇ Centre for Applied Cryptographic Research (CACR) — University of Waterloo
Cryptography Seminar Organizer — Spring 2008

◇ SecNet 2006, Annual Network Security Workshop — IIT-Bombay
Overall Coordinator — Spring 2006

University Activities

◇ Member, Graduate Admissions Committee, CS, Purdue University — Fall 2015–*present*

- ◇ Member, INSC Admission Committee, CERIAS, Purdue University — Spring 2016–*present*
- ◇ College of Science Team Award, Purdue University — Fall 2015
  Development work toward the professional masters degree concentration in information security
- ◇ Started the Crypto Reading Group, Purdue University — weekly, Spring 2016–*present*
- ◇ Started the Internet of Value Research meetings, Purdue University — weekly, Fall 2016–*present*
- ◇ Undergraduate Research Engagement
  Seminar Talk, CS 397 Honors Seminar, Purdue University — Fall 2015
  Seminar Talk, CS 397 Honors Seminar, Purdue University — Fall 2016

AWARDS AND HONORS

- ◇ **Best paper award** at ACM Conference on Online Social Networks (COSN 2015) — Nov 2015
- ◇ Nominated for a **Distinguished Dissertation Award** of the Canadian Association for Graduate Studies — Winter 2011
- ◇ **University of Waterloo Graduate Scholarship** — Winter 2008
- ◇ **David R. Cheriton Graduate Scholarship**, University of Waterloo — 2007–10
- ◇ **Technical Color** for excellence in technical activities by Computer Science and Engineering Association (CSEA), IIT-Bombay — 2005–06
- ◇ Competence in Software Technology **(CST) award** by the Centre for Development of Advanced Computing (C-DAC), India — 2004

OTHER SERVICES AND WORK

- ◇ Research Group Leaders' Representative at the MMCI Clusterboard, Saarland University — 2013-15
- ◇ Director Search Committee, School of Computer Science — University of Waterloo
  Graduate Students Representative — 2009-10
- ◇ Division Manager (Don) at Waterloo Co-op Residence Inc.(WCRI), Canada — Fall 2008
- ◇ Industrial Experience
  - · Member of Technical Staff, Persistent Systems Pvt. Ltd. (PSPL), India — Mar 2004–Jul 2004
  - · Trainee System Analyst, National Stock Exchange (NSE.iT), India — Aug 2003–Mar 2004

Aniket Kate
CS, Purdue University
December 2016